U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

March 24, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This responds to your letters, dated February 8 and February 24, 2006, posing questions to Attorney General Gonzales regarding the Terrorist Surveillance Program. The enclosed documents are responsive to all Majority and Minority questions your Committee submitted to the Department of Justice.

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable John Conyers
Ranking Minority Member

RESPONSES TO JOINT QUESTIONS FROM HOUSE JUDICIARY COMMITTEE MINORITY MEMBERS

Targets of Surveillance

1. Approximately how many persons located in the US have been targets of government intelligence activity under the warrantless surveillance program?

The National Security Agency ("NSA") electronic surveillance activities confirmed by the President involve targeting for interception by the NSA of communications where one party is outside the United States and there is probable cause ("reasonable grounds") to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization (hereinafter, the "Terrorist Surveillance Program" or the "Program"). Operational details about the scope of the Terrorist Surveillance Program are classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the scope of the Program could compromise its value by facilitating terrorists' attempts to evade it. We note, however, that consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

2. What criteria is used by NSA staff to determine whether one party to the communication is a person working in support of al Qaeda?

Under the Terrorist Surveillance Program, decisions about what communications to intercept are made by professional intelligence officers at the NSA who are experts on al Qaeda and its tactics, including its use of communications systems. Relying on the best available intelligence and subject to appropriate and rigorous oversight by the NSA Inspector General and General Counsel, among others, the NSA determines whether one party is outside of the United States and whether there is probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

3. Is the internal standard used to decide whether to monitor the communications of a person in the United States under the Program identical to the FlSA standard? In other words, before someone's communications are targeted for interception, does someone determine that there is probable cause to believe the target is knowingly conspiring with a foreign terrorist?

The Terrorist Surveillance Program targets communications only where one party is outside the United States and where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated

. . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). FISA also employs a probable cause standard (specifically, whether there is "probable cause to believe" that the target of the surveillance is an agent of a foreign power). *See* 50 U.S.C. § 1805(a)(3).

4. Once the NSA decides to monitor the communications of a person in the United States, do they also target and monitor the communications of any person in the United States who communicates with the original target? If so, does someone first determine whether the second target is knowingly conspiring with a foreign terrorist?

As set forth above, communications are targeted for interception under the Terrorist Surveillance Program only if one party is outside the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

Scope of NSA Program

5. How many hours and dollars have been spent searching or seizing the phone calls or emails of people in the US, and how much of this has been spent on people who have never been charged with any crime?

Operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. As noted above, consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

6. How many people in the US have been referred to the FBI for further inquiry or investigation? How many people whose emails or phone calls have been monitored have never been referred to the FBI?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

7. Are the names, phone numbers, or email addresses of persons in the United States who have had their communications monitored as part of the Program been included on any watch lists?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

Telecommunications Companies

8. Telecommunications companies and Internet Service Providers ("ISPs") are protected from criminal and civil liability if they are provided a court order from the FlSA court or criminal court or if a high-ranking DOJ official has certified in writing that "No warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." Has anyone at the Justice Department provided any telephone companies or ISPs with these certifications in the course of implementing the NSA's program?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore we cannot confirm or deny operational details of the program in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

9. Which telecommunications firms have opened American communications arteries to the NSA without a warrant?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore we cannot confirm or deny operational details of the program in this setting. Revealing information about the operational details of the Program could compromise its value by facilitating terrorists' attempts to evade it. Consistent with the notification provisions of the National Security Act, certain Members of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence have been briefed on the operational details of the Program.

Use of Information

10. To what extent has information collected included details of the targets' personal lives or political views, and has such information been immediately destroyed? Have intelligence agencies taken any actions beyond surveillance with regard to such individuals?

The purpose of the Terrorist Surveillance Program is to protect the Nation from foreign attack by detecting and preventing plots by a declared enemy of the United States that has already killed thousands of innocent civilians in the single deadliest foreign attack on U.S. soil in the Nation's history. In order to advance that end while simultaneously protecting civil liberties, procedures are in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

11. Was evidence obtained from the NSA classified surveillance program subsequently used to obtain a warrant from the FlSA court? If so, how many times has this occurred?

As we have explained above, operational information about the Terrorist Surveillance Program is classified and sensitive, and therefore cannot be discussed in this setting. Nor can we disclose the content of classified and sensitive communications and pleadings filed with the Foreign Intelligence Surveillance Court.

12. What is done with the information collected from the warrantless surveillance program that ends up not being useful for law enforcement or security purposes?

As indicated above, procedures are in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons. Those guidelines are designed to ensure that the Terrorist Surveillance Program is conducted in a manner consistent with preserving civil liberties.

13. Other than the President, what individuals at the White House are briefed on the program, and how often are they briefed?

The Terrorist Surveillance Program remains classified and highly sensitive. In general, the identity of individuals who have been briefed into the Program is also classified. We have previously explained, however, that the President sought legal advice prior to authorizing the Terrorist Surveillance Program and was advised that it is lawful, and that the Program has been reviewed by lawyers at the Department of Justice (including the Attorney General), by lawyers at the NSA, and by the Counsel to the President. Since 2001, the Program has been reviewed multiple times by different

counsel. Although the President is responsible for reauthorizing the Program, his determination to do so is based on reviews undertaken by the Intelligence Community and Department of Justice, a strategic assessment of the continuing importance of the Program to the national security of the United States, and assurances that safeguards continue to protect civil liberties. That process requires certain individuals to be cleared to receive classified and sensitive information about the Program.

14. When was James Baker read into the Program?

Please refer to the answer to question 13.

15. Who at the Department of Justice was informed of the Program? When?

Please refer to the answer to question 13.

16. When was the Solicitor General's office and the Deputy Attorney General's office informed of the program?

Please refer to the answer to question 13.

17. Does the Attorney General personally approve or authorize each interception of a United States person's communication? If not, who approves each interception?

As explained above, under the Terrorist Surveillance Program, professional intelligence officers at NSA, who are experts on al Qaeda and its tactics (including its use of communications systems), make the decisions about which international communications should be intercepted. Relying on the best available intelligence and subject to appropriate and rigorous oversight, those officers determine whether there is probable cause to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. In addition, the NSA, the Department of Justice, and the Office of the Director of National Intelligence conduct oversight of the Terrorist Surveillance Program through, for example, the reauthorization process.

18. Does anyone independent of the NSA check persons in the US whose phone calls or emails are searched or seized to make sure that they are not being targeted based on their political opinions?

General Hayden has stated that the Terrorist Surveillance Program is "overseen by the most intense oversight regime in the history of the National Security Agency," *see* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html, and is subject to extensive review in other departments as well. The oversight program includes review at the National Security Agency (by both the Office of General Counsel and Office of Inspector General) and the Department of Justice. In addition, with the participation of the Office of the Director of National Intelligence and the Department of Justice, the Program is reviewed

every 45 days, and the President decides whether to reauthorize it. This review includes an evaluation of the Terrorist Surveillance Program's effectiveness, a thorough assessment of the current threat to the United States posed by al Qaeda, and assurances that safeguards continue to protect civil liberties.

Minimization Procedure

19. Executive Order 12,333[] provides that intelligence agencies are only authorized to collect information on US persons consistent with the provisions of that Executive Order and procedures established by the head of the agency and approved the Attorney General. (Sec. 2.3). What minimization procedures are in effect concerning information gathered by the NSA concerning persons in the US?

Procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons. NSA applies minimization procedures that are appropriate and approved for the activity at issue. For example, special minimization procedures, approved by the Foreign Intelligence Surveillance Court, govern NSA handling of U.S. person information acquired pursuant to FISA-authorization surveillance. Department of Defense Regulation 5240.1-R (and its classified annex) are the guidelines approved by the Attorney General that are referred to in Executive Order 12333. Those guidelines govern NSA's handling of U.S. person information. United States Signals Intelligence Directive 18 provides more detailed guidance on the latter.

20. Has United States Signals Intelligence Directive [USSID] 18, "Legal Compliance and Minimization Procedures," July 27, 1993, applicable to the NSA, been changed since January 2001? Is it still in effect? Does that Directive, as amended or not, apply to all surveillance being undertaken by the NSA of persons inside the US outside of the procedures set forth in FISA?

United States Signals Intelligence Directive 18 has not been changed since January 2001 and is still in effect. As indicated above, procedures are in place under the Terrorist Surveillance Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

21. When were the minimization procedures last changed? Did the Attorney General approve those changes? When?

Executive Order 12333 calls for Attorney General-approved procedures for the collection, retention, and dissemination of information concerning U.S. persons. The Secretary of Defense issued the current version of these procedures in December 1981

applicable to all Department of Defense ("DoD") intelligence agencies. The Attorney General signed those procedures in October 1982. A classified annex to those procedures dealing specifically with signals intelligence was promulgated by the Deputy Secretary of Defense in April 1988 and approved by the Attorney General in May 1988. NSA has internal procedures derivative of those authorities that were last updated in 1993. The annex that specifically governs FISA procedures was modified, with Attorney General Reno's approval, in 1997.

22. When was the last time you supplied any Member of the House Judiciary Committee or any Committee of the Congress a copy of such minimization procedures?

NSA has briefed intelligence committees of both Houses extensively on minimization procedures over the past several years. NSA can determine from available records only that NSA provided Senate Select Committee on Intelligence staff DoD Regulation 5240.1-R and its classified annex in January 2006 and both USSID 18 and DoD Regulation 5420.1-R and its annex in July 2005. NSA's records do not indicate when a copy of those materials was last provided to the House Permanent Select Committee on Intelligence. However, it is important to note that much of this material is freely available. USSID 18, July 27, 1993, has been made publicly available in redacted form (*see, e.g.*, www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm). In addition, DoD Regulation 5240.1-R, December 1982 (but not its annex) has been declassified and made publicly available (*see, e.g.*, http://cryptome.org/dod5240-1r.htm).

Concerns About the NSA Program from Within the Administration

23. How many federal employees have expressed concerns about or objections to this program and what has been done regarding those employees of the NSA or other federal agencies or in response?

It would be inappropriate for us to disclose any confidential internal deliberations of the Executive Branch. The long-recognized confidentiality protections afforded Executive Branch communications are designed to encourage candid advice from Executive Branch lawyers and officers, and subjecting such advice to disclosure would chill those deliberations. The General Counsel and Inspector General of the NSA oversee the NSA's implementation of the Terrorist Surveillance Program. We note that there are procedures in place under the Intelligence Community Whistleblower Protection Act of 1998 that permit employees concerned about the legality of intelligence programs to report their concerns to the inspectors general of intelligence agencies and thence to Congress.

24. Why was the NSA program suspended in 2004?

The Terrorist Surveillance Program described by the President has never been suspended; it has been in operation since its inception in October 2001. Indeed, the President explained that he intends to reauthorize that Program as long as the threat posed

by al Qaeda and its allies justifies it. Beyond this, we cannot discuss the operational details or history of the Terrorist Surveillance Program. Nor can we divulge the internal deliberations of the Executive Branch.

Presidential Claim of Inherent Authority

25. What is the limiting principle of the President's claimed inherent authority as commander-in-chief? For example, does this interpretation of the law authorize the opening of first-class mail of U.S. citizens under the DOJ's interpretation, and if not, why not?

The Terrorist Surveillance Program intercepts only communications where one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not include the opening of first-class United States mail. There is a long history of Presidents, including Woodrow Wilson and Franklin Roosevelt, authorizing the interception of international electronic communications during times of armed conflict as an exercise of the President's inherent authority under the Constitution and pursuant to general force authorization resolutions. Whether the President's authority under the Constitution would permit the interception of mail would require a different legal analysis. In light of the strictly limited nature of the Terrorist Surveillance Program, we do not think it a useful or a practical exercise to engage in speculation about the limits of the President's authority as Commander in Chief. *Cf. Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("The actual art of governing under our Constitution does not and cannot conform to judicial definitions of the power of any of its branches based on isolated clauses or even single Articles torn from context.").

26. Under the Administration's legal interpretation, does the President have the authority to wiretap Americans' domestic calls and emails under his inherent constitutional power and the AUMF, if he feels it involves al Qaeda activity?

The Force Resolution's authorization of "all necessary and appropriate force," which the Supreme Court in *Hamdi* interpreted to include the fundamental and accepted incidents of the use of military force, clearly encompasses the narrowly focused Terrorist Surveillance Program. There is a long history of Presidents authorizing the interception of *international* electronic communications during a time of armed conflict. President Wilson, for example, relying only on his constitutional powers and a general congressional authorization for use of force, authorized the interception of *all* telephone, telegraph, and cable communications into and out of the United States during World War I. *See* Exec. Order 2604 (Apr. 28, 1917). Similarly, President Roosevelt authorized the interception of "*all . . . telecommunications traffic* in and out of the United States." As explained in the Justice Department's paper of January 19, 2006, that historical foundation lends significant support to the President's authority to undertake the Terrorist Surveillance Program under the AUMF and the Constitution; indeed, the Program is much narrower than the interceptions authorized by either President Wilson or President

Roosevelt. Interception of the content of domestic communications would present a different legal question.

Authorization for Use of Military Force (AUMF)

27. When did the Administration and DOJ decide that the Authorization for Use of Military Force (AUMF) granted the Administration the power to create the NSA program?

The Department has reviewed the legality of the Terrorist Surveillance Program on multiple occasions. We cannot discuss the operational details or history of the Terrorist Surveillance Program.

28. Are there any other actions under the AUMF that, without the President's inherent constitutional power, would not be permitted because of the FlSA statute? Are there any programs currently being used like that?

We are not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program, though our inability to respond should not be taken to suggest that there are such activities. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

29. Under the Administration's interpretation of AUMF, has the President ever invoked his authority as commander-in-chief through either secret order or directive other than NSA surveillance?

As stated above, we are not in a position to provide information here concerning any other intelligence activities beyond the Terrorist Surveillance Program, though our inability to respond should not be taken to suggest that there are such activities. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

30. How do you reconcile the Attorney General's statement that Congress would not have granted the Executive such authority and at the same time, contend that this authority is something that Congress intended to give under the AUMF?

We understand your question to be a reference to a statement the Attorney General made on December 19, 2005. As the Attorney General clarified both later in the same December 19th briefing and on December 21, 2005, it is not the case that the Administration declined to seek a specific authorization of the Terrorist Surveillance Program because we believed Congress would not authorize it. *See* Remarks by

Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act, *available at* http://www.dhs.gov/dhspublic/display?content=5285. Rather, as the Attorney General testified before the Senate on February 6, 2006, the consensus view in discussions with Members of Congress was that it was unlikely, if not impossible, that more specific legislation could be enacted without compromising the Terrorist Surveillance Program by disclosing operational details, limitations, and capabilities to our enemies. Such disclosures would necessarily have compromised our national security.

Foreign Intelligence Surveillance Act (FISA)

31. When did the Administration reach the conclusion that FISA did not have to be followed to use the NSA program?

Before answering this question, we note that the Department's legal analysis assumes, solely for purposes of that analysis, that the targeted interception of international communications authorized under the President's Terrorist Surveillance Program would constitute "electronic surveillance" as defined in FISA. As noted in our January 19th paper, we cannot confirm whether that is actually the case without disclosing sensitive classified information.

As explained at length in the Justice Department's paper of January 19, 2006, the Terrorist Surveillance Program is completely consistent with FISA. FISA itself includes an exception for surveillance "authorized by statute," 50 U.S.C. § 1809(a). In light of the decision in *Hamdi v. Rumsfeld* that the AUMF authorizes the President to undertake fundamental and accepted incidents of war and the long history demonstrating that signals intelligence against the enemy is such a fundamental incident of war, the AUMF is a statute that authorizes intelligence surveillance against members and agents of al Qaeda and affiliated terrorist organizations and thereby satisfies FISA.

The President was advised that the Terrorist Surveillance Program was lawful before he first authorized it in October 2001.

32. Did the increasing number of modified and rejected requests for FISA warrants since 2001 implicate the Administration's determination to bypass FISA?

As explained above, the Terrorist Surveillance Program does not "bypass FISA."

The determination to implement the Terrorist Surveillance Program was made based on the advice of intelligence experts that the Nation needed an early warning system, one that could help detect and prevent another catastrophic al Qaeda attack. The President authorized the Terrorist Surveillance Program because it offers the speed and agility required to defend the United States against further terrorist attacks by al Qaeda and affiliated terrorist organizations. Among the advantages offered by the Terrorist Surveillance Program compared to FISA is *who* makes the probable cause determination

and how many layers of review will occur *before* surveillance begins. Under the Terrorist Surveillance Program, professional intelligence officers, who are experts on al Qaeda and its tactics (including its use of communications systems), with appropriate and rigorous oversight, make the decisions about which international communications should be intercepted. By contrast, because FISA requires the Attorney General to "reasonably determine[]" that "the factual basis for issuance of" a FISA order exists at the time he approves an emergency authorization, *see* 50 U.S.C. § 1805(f)(2), as a practical matter, it is necessary for NSA intelligence officers, NSA lawyers, Justice Department lawyers, and the Attorney General to review a matter before even emergency surveillance would begin. Great care must be exercised in reviewing requests for emergency surveillance because of the risks involved. Among other things, if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, there is a risk that the court would disclose the surveillance to U.S. persons whose communications were intercepted, *see* 50 U.S.C. § 1806(j), potentially compromising ongoing intelligence efforts. In the narrow context of defending the Nation in this congressionally authorized armed conflict with al Qaeda, we must allow these highly trained intelligence professionals to use their skills and knowledge to protect us.

33. Do you know of any other President who has authorized warrantless wiretaps outside of FlSA since FlSA was passed in 1978? If so, please explain.

The laws of the United States, both before and after FISA's enactment, have long permitted various forms of foreign intelligence surveillance, including the use of wiretaps, outside the procedures of FISA. If the question is limited to "electronic surveillance" as defined by FISA, however, we are unaware of such authorizations.

34. In a press briefing on December 19, 2005, General Hayden stated that the NSA was using a subtly softer trigger which precluded going to the FISA court. What exactly constitutes this softer trigger?

As noted above, the "reasonable grounds to believe" standard is a "probable cause" standard of proof. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("We have stated . . . that '[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.'"). FISA also employs a probable cause standard (specifically, whether there is "probable cause to believe" that the target of the surveillance is an agent of a foreign power). *See* 50 U.S.C. § 1805(a)(3). The relevant distinction between the two methods—and the critical advantage offered by the Terrorist Surveillance Program compared to FISA—is the greater speed and agility it offers.

35. How many FISA judges were informed of the warrantless surveillance program?

The Terrorist Surveillance Program remains classified and sensitive. In general, the identity of individuals who have been briefed into the Program is also classified. In addition, we cannot disclose the content of our discussions with the Foreign Intelligence

Surveillance Court. We assure you, however, that the Department keeps the Foreign Intelligence Surveillance Court fully informed regarding information that is relevant to the FISA process.

36. Was any judge on the FISA court of review informed of the NSA program as part of the briefing of the 2002 appellate case, *In re Sealed Case*? Were any of the lawyers on that case read into the program? How many?

As we noted above, the identity of individuals who have been briefed into the Terrorist Surveillance Program is generally classified. We note, however, that *In re Sealed Case*, 310 F.3d 717 (For. Int. Surv. Ct. Rev. 2002), involved whether the FISA Court had statutory or constitutional authority to place restrictions on interaction of criminal prosecutors and foreign intelligence investigators as a condition for granting surveillance orders. The Terrorist Surveillance Program would not have been relevant to the question before the court in that case.

37. Are there currently any plans to take the entire NSA program to the FISA Court within the broad parameters of what is reasonable and constitutional and ask the FlSA Court to approve it or disapprove it? If not, why not?

It would be inappropriate to discuss here future plans for seeking any particular order from the Foreign Intelligence Surveillance Court, which could involve both privileged internal Executive Branch communications and deliberations and classified and sensitive court filings. The Department has, however, sought to use the FISA process wherever possible, and we will continue to consider all lawful options.

38. What aspects of FISA are too burdensome for the Administration to comply with? Why did the Administration fail to utilize the emergency provision of FISA?

As noted above, the determination was made, based on the advice of intelligence experts, that the Nation needed an early warning system to help detect and prevent another catastrophic al Qaeda attack. Speed and agility are critical in this context. It would be an unjustifiable lapse if al Qaeda electronic communications were used to coordinate another deadly attack on America, but the communications were not intercepted in time because of the delay that traditional FISA procedures require.

The emergency authorization provision in FISA, which allows 72 hours of surveillance without obtaining a court order, does not—as many believe—allow the Government to undertake surveillance immediately. Rather, in order to authorize emergency surveillance under FISA, the Attorney General first must personally "determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists." 50 U.S.C. § 1805(f). FISA requires the Attorney General to determine that this condition is satisfied *in advance* of authorizing the surveillance to begin. The process needed to make that determination, in turn, can take time. Section 106(j) of FISA, 50 U.S.C. § 1806(j), provides that if a court later declines to authorize an

interception that previously was authorized by the Attorney General under the so-called "emergency" exception to FISA, it may order disclosures about the surveillance to U.S. persons whose communications were intercepted. Thus, using the "emergency" exception poses a risk that surveillance activities will be subject to public disclosure. To reduce that risk, the Attorney General follows a multi-layered procedure before authorizing interception under the "emergency" exception to help to ensure that any eventual application will be approved by the Foreign Intelligence Surveillance Court. That process ordinarily entails review by intelligence officers at the NSA, NSA attorneys, and Department of Justice attorneys, each of whom must be satisfied that the standards have been met before the matter proceeds to the next group for review. Compared to that multilayered process, the Terrorist Surveillance Program affords a critical advantage in terms of speed and agility.

Miscellaneous

39. According to the Administration, a line NSA analyst rather than an independent judge determines whether or not an intrusion into a[] citizen's privacy is reasonable. Do you think that there are appropriate checks and balances under this framework?

Yes. As noted earlier, General Hayden has stated that the Terrorist Surveillance Program is "overseen by the most intense oversight regime in the history of the National Security Agency," *see* Remarks by General Michael V. Hayden to the National Press Club, *available at* http://www.dni.gov/release_letter_012306.html, and is subject to extensive review in other departments as well. Please refer to the answer to question 18 for further information about the considerable privacy protections that are built into the Program.

40. Have any purely domestic calls intercepted through the NSA program? What happens if such calls are intercepted, to the information and the responsible employee?

The Terrorist Surveillance Program targets for interception only those communications where one party is outside of the United States and there is probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. The Program does not target for interception wholly domestic communications (*i.e.*, communications which both originate and terminate within the United States). There are procedures in place to avoid the interception of domestic calls. In addition, as mentioned above, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

41. Is the NSA engaged in keyword analysis or pattern analysis of purely domestic communications?

The Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. It would be inappropriate to discuss in this setting the existence (or non-existence) of specific intelligence activities or the operations of any such activities other than the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

42. Is the NSA engaged in keyword analysis or pattern analysis of the communications of people in the United States who call or email overseas?

As noted above, the Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. It would be inappropriate to discuss in this setting the existence (or non-existence) of specific intelligence activities or the operations of any such activities other than the Terrorist Surveillance Program. Consistent with long-standing practice, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the oversight committees and, in certain circumstances, congressional leadership.

43. Has information obtained through warrantless NSA interceptions been used in any criminal prosecutions?

The purpose of the Terrorist Surveillance Program is not to bring criminals to justice. Instead, the Program is directed at protecting the Nation from foreign attack by detecting and preventing plots by a declared enemy of the United States. Because the Program is directed at a "special need, beyond the normal need for law enforcement," the warrant requirement of the Fourth Amendment does not apply. *See*, *e.g.*, *Vernonia School Dist. v. Acton*, 515 U.S. 646, 653 (1995). Because collecting foreign intelligence information without a warrant does not violate the Fourth Amendment and because the Terrorist Surveillance Program is lawful, there appears to be no legal barrier against introducing this evidence in a criminal prosecution. *See* 50 U.S.C. § 1806(f), (g). Past experience outside the context of the Terrorist Surveillance Program indicates, however, that operational considerations, such as the potential for disclosing classified information, must be considered in using intelligence information in criminal trials.

44. Are their any plans by the Bush administration to inform those US individuals whose phone calls or emails were searched or seized but they have been cleared of any wrongdoing?

As explained above, the Terrorist Surveillance Program is subject to rigorous oversight to protect privacy interests. In addition, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.

45. Are any communications between attorneys and their clients or doctors and patients being captured?

The Terrorist Surveillance Program targets communications for interception only when one party is outside the United States and there is probable cause to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. Although the Program does not specifically target the communications of attorneys or physicians, calls involving such persons would not be categorically excluded from interception if they met these criteria. As mentioned above, however, procedures are in place to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, that govern acquisition, retention, and dissemination of information relating to U.S. persons.